УДК 343.98

Д. И. Шнейдерова
преподаватель кафедры уголовного процесса и криминалистики
Могилевского института МВД Республики Беларусь

УСТАНОВЛЕНИЕ ПРИНАДЛЕЖНОСТИ ЛИЦУ КРИПТОКОШЕЛЬКА ПО ДЕЛАМ О ХИЩЕНИЯХ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ: КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ

Криптовалюты, благодаря своим функциональным особенностям, способам обращения и эмитирования, за последние несколько лет прочно укрепились в качестве универсального цифрового средства платежа, обмена и инвестирования, сформировав обширный блок сфер своего распространения и многочисленную пользовательскую базу. В свою очередь, преимущества криптовалют были отмечены не только добросовестными пользователями, но и киберпреступниками, разработавшими ряд успешно применяемых схем по хищению криптовалют путем мошенничества, вымогательства и модификации компьютерной информации.

На стадии возбуждения уголовных дел о хищениях в сфере оборота криптовалют и на первоначальном (последующем) этапе их расследования правоохранительные органы сталкиваются с рядом проблем, одной из которых выступает вопрос доказывания принадлежности определенных криптовалют и криптовалютных кошельков конкретному пользователю (потерпевшему — на стадии возбуждения и первоначального этапа расследования, подозреваемому — на последующем этапе). Например, при поступлении от гражданина заявления о незаконном списании с его криптовалютного кошелька определенного количества криптомонет в первую очередь необходимо убедиться, что заявляемый кошелек действительно принадлежит обратившемуся лицу. Знания адреса кошелька и входных данных, которые, как правило, предоставляет заявитель, недостаточно, чтобы судить и о принадлежности ему кошелька, и о наличии факта хищения из него криптовалют.

Центральным объектом исследования при установлении принадлежности криптокошелька потерпевшему или подозреваемому выступает пользовательское устройство (компьютер, планшет, смартфон), изучение содержимого которого способствует выявлению цифровых следов, доказывающих владение криптокошельком и криптовалютами. Исследование устройства возможно в рамках осмотра места происшествия с участием специалиста в IT-сфере, при изъятии системного блока, мобильного устройства и съемных накопителей

памяти, аппаратных кошельков в ходе обыска или выемки с последующим назначением компьютерно-технической экспертизы.

В ходе указанных следственных действий специалистом (экспертом) могут быть выявлены следующие следственные индикаторы, свидетельствующие о взаимодействии владельца устройства как с криптовалютами в целом, так и с определенным криптовалютным кошельком: локальное программное обеспечение для хранения криптовалют и совершения сделок с ними (программные криптокошельки, программы для авторизации и синхронизации аппаратных кошельков); история браузера с журналом загрузок файлов (программные файлы для работы с криптовалютой, файлы с вирусными программами-вымогателями / шпионами) и журналом посещения веб-страниц (среди которых могут быть выявлены сайты онлайн-кошельков, криптобирж и обменников, торговых площадок, производящих расчет через криптовалюты, фишинговые сайты крипторесурсов, ссылки к облачному хранилищу и т. д.); менеджер паролей (сохраненные логины и пароли для доступа к онлайн-криптокошельку, облачному хранилищу, учетные данные аккаунтов на криптобиржах и обменниках); текстовые и графические файлы с сохраненными открытыми и приватными ключами для совершения транзакций с криптовалютой определенного кошелька, QR-кодами для доступа к криптокошелькам), системные файлы работы на устройстве с определенными программами; второй windows-клиент, где пользователь осуществлял работу исключительно с криптовалютой, а для иных целей пользовался основной учетной записью в операционной системе; на смартфоне — приложения для хранения, покупки и обмена криптовалют, СМС-сообщения аутентификации.

Пользовательское устройство является не единственным источником информации, связывающим конкретного пользователя с криптокошельком и похищенной криптовалютой. В рамках оперативной и следственной работы должны быть исследованы интернет-трафик, связанный с определенным устройством, что может способствовать не только доказыванию принадлежности кошелька потерпевшему, но и установлению устройства подозреваемого, связь банковских карт потерпевшего и подозреваемого с криптобиржами и криптообменниками, а также через поисковые запросы в сети Интернет должен быть проанализирован адрес криптокошелька, в том числе с использованием криптоанализаторов и обозревателей.

Анализ интернет-трафика возможен при получении требуемой информации через запрос от оператора сети, предоставляющего услуги интернет-соединения проверяемому пользователю (потерпевшему или подозреваемому). Для формирования такого запроса необходимы первоначальные сведения либо

о самом пользователе (анкетные данные, адрес места жительства), либо об используемом им устройстве (в частности, IP-адрес компьютера или смартфона). При этом в рамках исследования входящего и исходящего трафика можно установить, с какими устройствами и серверами взаимодействовал пользовательский компьютер или смартфон, определить их IP-адреса, характер взаимодействия, факт передачи данных и файлов, но определить внутреннее содержимое файлов без доступа к месту их хранения не представляется возможным. Следовательно, данные трафика сети способствуют подтверждению факта связи устройства пользователя с серверами криптовалютных сервисов (кошельки, обменники, биржи, распределительные реестры) в области управления аккаунтами, что может свидетельствовать о принадлежности определенного криптокошелька проверяемому лицу, а также поможет установить стороннее вмешательство третьих лиц к памяти устройства. Однако могут возникнуть затруднения в случаях, если пользователь использовал сервисы для анонимного сетевого соединения (например, браузеры VPN или Tor), которые заменяют реальный IP-адрес на адрес сервера такого сервиса, и обращаться с запросами уже необходимо к его владельцам.

В случае если пользователь приобретал или обналичивал криптовалюту с использованием фиатных денежных средств в безналичной форме, появляется возможность установить привязку банковских карт лица с аккаунтом на криптобирже, обменнике или к криптокошельку, взаимодействующему с указанными сервисами, что свяжет определенного пользователя с адресом кошелька. Также эффективным представляется способ поиска информации о криптокошельке через поисковые системы Google, DuckDuckGo и другие, которые позволят выявить такие индикаторы связи криптокошелька и человека, как аккаунты в социальных сетях и на торговых площадках, электронную почту, номер мобильного телефона, записи в блогах и на форумах, фотографии, видеоролики, иные общедоступные источники, где пользователь хотя бы единожды публиковал адрес кошелька [1].

Таким образом, в рамках криминалистической методики расследования хищений в сфере оборота криптовалют можно выделить четыре способа, позволяющих связать конкретную личность с адресом криптокошелька и похищенными монетами: исследование пользовательского устройства, анализ интернет-трафика, установление факта использования банковских карт для покупки или обналичивания криптовалют, анализ сведений публичного доступа об адресе кошелька через поисковые запросы и блокчейн-анализаторы.

Список основных источников

1. Использование общедоступных источников информации для деанонимизации криптовалютных кошельков [Электронный ресурс] // Habr. — Режим доступа: https://habr.com/ru/company/tomhunter/blog/579180/. — Дата доступа: 03.02.2022. Перейти к источнику Вернуться к статье